⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平4－155471

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成4年(1992)5月28日
G 06 F 15/30	350	6798－5L	
15/21	340 C	7218－5L	
		8111－3E　G 07 F 7/08	C※

審査請求　未請求　請求項の数 1　（全8頁）

㊹発明の名称　取引認証方式

㉑特　願　平2－279390
㉒出　願　平2(1990)10月19日

⑫発明者　岩井　尚史　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内
⑫発明者　熊井　康子　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑫発明者　小林　孝文　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑪出願人　沖電気工業株式会社　東京都港区虎ノ門1丁目7番12号
⑪出願人　エヌ・テイ・テイ・データ通信株式会社　東京都港区虎ノ門1丁目26番5号
⑭代理人　弁理士　鈴木　敏明

最終頁に続く

明　細　書

1．発明の名称

取引認証方式

2．特許請求の範囲

ＩＣカードをＩＣカードオフラインターミナルに挿填し、取引認証を行なう取引認証方式において、

上記ＩＣカードは、個人識別用暗証番号データ、データ列を暗号化する第1のコード、データ列を暗号化する第2のコード、及びデータ列を暗号化する第3のコードが記録され、

上記ＩＣカードオフラインターミナルは、前記第1のコード及び前記第2のコードと同一コードが記録され、

前記ＩＣカードが作成した第1のデータ列を前記ＩＣカード及びＩＣカードオフラインターミナルの両方で前記第1のコードによりスクランブルし、該スクランブルした両方のデータの一致を検出する手段と、

前記ＩＣカードオフラインターミナルが作成した第2のデータ列を、前記ＩＣカードオフラインターミナル及びＩＣカードの両方で前記第2のコードによりスクランブルし、該スクランブルした両方のデータの一致を検出する手段と、

前記オフラインターミナルに入力された暗証番号と、前記暗証番号データの一致を検出する手段と、

金融機関から送信された取引認証用のデータを前記オフラインターミナルに入力し、前記第3のコードによりスクランブルし、前記金融機関に送信する手段と、

前記金融機関にて受信した前記第3のコードによりスクランブルされた取引認証用データと、前記取引認証用のデータを該金融機関に記録された前記第3のコードと同一コードによりスクランブルされたデータとの一致を検出する手段とを有する取引認証方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は、例えば銀行等の金融機関、あるいは

クレジット会社等によって発行されるキャシュレスカードを用いて取引を行う場合に、確実に、取引認証をおこなう取引認証方式に関する。

〔従来の技術〕

近年は、キャシュレス時代と呼ばれており、クレジット会社などに依り発行されたカードを使用することに依り、現金の取扱をせずに商品の購入が可能となっている。上記カードとしては、従来、プラスチックカード、エンボスカード、磁気ストライプカードなどが一般に使用されているが、これらのカードは構造上偽造が簡単であり、不正使用が問題となっている。このような問題を解決するため、最近ではカード内に、暗証番号等を記憶したＩＣ回路を組み込み、暗証番号が外部から容易に読み出せないようにした情報カード、いわゆるＩＣカードが開発されている。このＩＣカードは、偽造が困難で、機密性に優れ、又、多数の情報を記憶できるという利点がある。しかして、上記のようなＩＣカードを使用して実際に取引を行う場合には、銀行あるいは商店などに設置したICカードターミナルにＩＣカードを装着し、暗証番号などを入力してカードおよびカード所有者の正当性を確認したのち所定の取引動作が行われるようにしている。

〔発明が解決しようとする課題〕

しかしながら、このようにＩＣカードをターミナルに装着して暗証番号の照合を行う場合、第一に、例えば、商店などにおいて暗証番号の入力を行う際にその入力操作自体を視覚によって盗まれる可能性がある。又、第二に、例えば、ターミナル側に、カード所有者によって入力される暗証番号の情報を、暗証番号一致の信号を持って記憶する細工が施してある場合、真のカード所有者の暗証番号が上記ターミナルの設置される商店主等によって簡単に盗まれてしまう恐れもある。

そこで現在、カード所持者の暗証番号をカード発行時において予めカード内メモリに記憶させ、カード本体に設けたキーボードより入力される暗証番号と、上記メモリ内暗証番号とを比較照合し、その照合結果を即座にＩＣカード自体に設けた表示部にて表示するようにした、所謂、ターミナル側とはまったく接続関係を持たないで、独自に本人照合を行うことのできるＩＣカードが考えられている。しかし、このような単独にて本人照合を行える機能を有するＩＣカードであっても、そのカード自体が偽造される可能性がある。すなわちカード本体上の表示部にて、例えば、「本人ＯＫ」などの表示が行われたとしても、そのカード自体真に正当なカード会社から発行されたものかどうかを確認できないため、結局、真のカード所有者の認証を行うのは非常に困難なものとなる。

又、取引が成立した場合、金融会社と、商店との間で取引を確認する情報は、商品の購入金額、取引銀行口座番号、領収書の通し番号などを、特定の暗号コードでスクランブル化して得られるものであるが、上記情報は、通常、金融会社等と商店との文書での取引確認用に用いられるものであってその場での取引の確認にはなんら役にたっていない。

〔課題を解決するための手段〕

本発明は、上記のような問題点に鑑みなされたもので、カード所有者の暗証情報が不正に盗まれることなく、カード所持者と金融会社の相互の正当性を確実に認証する、取引認証システムを提供することを目的とする。

すなわちこの発明に係わる携帯型ＩＣカードターミナルを用いた取引認証システムは、カード所有者特定用のデータをあらかじめ記憶させた個人証明カードを、携帯型ＩＣカードターミナルに接続させ、カードとターミナルで相互認証を行いカードとターミナルの正当性を確認し、上記カード所有者にて入力される所有者特定用のデータと上記カード内カード所有者特定用データを比較照合し、本人の正当性を確認するとともに、商品の購入金額、クレジットの会員番号等を、金融会社等に送付し、それを基にして得られるデータを金融会社のホストコンピュータと携帯型ＩＣカードターミナルの双方で、同一キー、同一アルゴリズムにてスクランブル化し、比較照合し、カード、ターミナルの正当性を金融会社のホストコンピュー

タで確認し、取引の正当性を認証するように構成したものである。

〔作　用〕

本発明は、ＩＣカード及びＩＣカードターミナルの双方に共通する第１及び第２のコードで、ICカードにて作成した第１のデータ列とＩＣカードリーダで作成した第２のデータ列をスクランブル化するため、ＩＣカードとＩＣカードリーダそれぞれが正当であることを確認するとともに、暗証番号にて持主とＩＣカードとの関係が正当であると確認できる。更に、金融機関から送信された取引認証用データを第３のコードでスクランブルするとともに、金融機関においても同一の第３のコードでスクランブルするので、ＩＣカードターミナルと金融機関との関係も正当であると確認できる。従って、上記全ての確認を行うことによりICカード持主から金融機関に至る全ての関係が正当であると確認できるのである。

〔実施例〕

以下図面によりこの発明の一実施例を説明する。

第２図はそのＩＣカードオフラインターミナルを具体化した場合のカードターミナル１１に点線で示すＩＣカード１２を装着した状態の概観構成図である。このカードターミナル１１は、その本体上面にキーボード１３および表示部１４を有し、キーボード１３の下側面にはＩＣカード１２との電気的接続を図るためのカード挿入口１５を有する。キー入力部１３は、テンキー、ファンクションキー１６などを備えている。ファンクションキー１６には、暗証番号ＰＩＮ（Personal Identification Number）や、取引認証番号ＳＡＮ(SalesApproval No.)を得るためのデータの入力終了を指示するＥＮＴＥＲキー（ＥＮＴ）や、カード内部に、取引手順が複数格納されている場合に、必要な取引を指定するためのカーソル移動キー（↑、↓）などがある。

次に、第３図は、上記カードターミナル１１にＩＣカード１２を装着した状態でのＡ１－Ａ２線縦断面構成を示すものである。カードターミナル１１は、回路基板２１と、この回路基板２１の下面側に設けられた中央制御部２２、相互／取引認証部２５、音声出力装置（スピーカ）２４、ＩＣカード１２との接続を図るための接続端子２３を有する。一方表示部１４は、液晶表示板２６を有して構成されている。

次に、第１図に依り、上記ＩＣカード１２の回路構成について説明する。

ＩＣカード１２は、中央制御部３１と、この中央制御部３１に接続された、データメモリ３２、ＰＩＮ照合部３４、相互認証部３３、及びインターフェース部３５と、インターフェース部３５に接続された接続端子３６とから構成される。データメモリ３２には、ＩＣカード１２の発行時において、カード所有者本人が設定した暗証番号PIN、ＩＣカード１２とカードターミナル１１の相互認証時に使用される暗号コード１、暗号コード２、取引認証番号生成に使用される暗号化コード３、および、本システムでの取引手順があらかじめ記憶されるとともに、例えば、商品取引に関する購入金額等のデータがその取引年月日とともに記憶するために用いる記憶エリアが確保される。PIN照合部３４は、カードターミナル１１にて本人照合を行う際には、カード所有者にてキー入力される暗証番号ＰＩＮと、上記データメモリ３２にてあらかじめ記憶される真のカード所有者のＰＩＮとを比較照合するものである。この照合部３４によりＰＩＮ一致と判定された場合には、上記カードターミナル１１に対して本人ＯＫのメッセージが送信される。相互認証部３３は、カードターミナル１１から送信される第１の乱数を、暗号コード１でスクランブルし上記カードターミナル１１に対して送信するとともに、第２の乱数を生成し、上記カードターミナル１１に対して送信する。カードターミナル１１、この、第２の乱数を、暗号コード２でスクランブルし、ＩＣカード１２に送信する。暗号コード１でＩＣカード１２でスクランブルされた乱数と、上記カードターミナル１１でスクランブルした乱数が一致すれば、上記カードターミナル１１からは、上記ＩＣカード１２は、同一の暗号コード１をもつ、正当なＩＣカードと

見なすことができる。一方、上記ＩＣカード１２が送信した第２の乱数を上記カードターミナルでスクランブルした乱数と、第２の乱数を上記ＩＣカード１２内で暗号コード２でスクランブルした乱数が上記ＩＣカード１２内で一致すれば、上記ＩＣカード１２からは、上記カードターミナル11は、同一の暗号コード２をもつ、正当なカードターミナルと見なすことができ、上記カードターミナル１１に対して認証ＯＫのメッセージが送信される。この様にして、カードターミナルに対するＩＣカード及びＩＣカードに対するカードターミナルの両方の相互認証処理を行なう。ここで、上記データメモリ３２はＥＥＰ－ＲＯＭにて構成可能である。

次に第４図により上記カードターミナル１１の回路構成について説明する。

カードターミナル１１は中央制御部２２と、この中央制御部２２に接続された、キー入力部１３を制御するキー入力制御部４１、表示部１４を制御する表示制御部４２、及びスピーカ２４を制御する音声出力制御部５０を有する。更に、中央制御部２２には、演算部４３と、インターフェース部４９を介してＩＣカード用接続端子２３と相互／取引認証部４４が接続される。上記相互／取引認証部４４は、上記インターフェース部４９介して中央制御部２２からのコマンドを実行するもので、取引認証番号生成部４５、相互認証部４６、制御演算部４７、データメモリ４８が備えられている。メモリ４８には、相互認証処理用の暗号コード１及び暗号コード２が記憶されている。相互認証処理の場合、上記インターフェース部４９を介して上記相互／取引認証部４４に相互認証コマンドが送信されると、上記相互／取引認証部４４の上記相互認証部４６のプログラムが起動され、上記メモリ４８の暗号コード１及び２を用いて、インターフェース部４９を介してＩＣカード１２との間で前述した相互認証処理を行い、お互いに正当であると認められた場合には、上記インターフェース部４９を介して上記中央制御部２２に相互認証ＯＫのメッセージを送信する。

取引認証番号生成部４５は、後述する様に、相互認証、ＰＩＮ照合後、本取引を行なう際に用いるもので、キー入力部１３から入力された取引認証番号生成番号と、ＩＣカード１２のデータメモリ３２より読み出した暗号化コード３を用いてスクランブルすることにより取引認証番号を生成するものである。この取引認証番号は、インターフェース部４９を介して、中央制御部２２に送信される。

次に、上記のように構成されるＩＣカードオフラインターミナルを用い、ＩＣカード１２による商品取引の際に、その場でカード取引認証番号を算出表示する動作を５図に示すフローチャートを用いて説明する。

まず、カード所有者は、商品の購入を行うに際して、商品との間で取引が成立すると、上記カードターミナル１１のカード挿入口１５に対してICカード１２を挿入する。すると、ＩＣカード１２は、第３図で示したように、カードターミナル11のカード装着部に装着され、カード側の接続端子３６とＩＣカード用接続端子２３が接続状態となる。ここで、中央制御部２２は、ステップＳ１において、相互認証コマンドをインターフェース部４９を介して相互／取引認証部４４に送信する。相互／取引認証部４４は、相互認証プログラム46を起動し、相互認証プログラム４６に従って第１の乱数を生成する。生成された第１の乱数は、インターフェース部４９およびＩＣカード用接続端子２３を介してＩＣカード内の相互認証部３３に送られる。又、インターフェース部４９を介してメモリ４８に記憶されている相互認証用暗号コード１を用いてスクランブル化され、メモリ４８に記憶される。一方、インターフェース部４９およびＩＣカード用接続端子２３を介して送られた第１の乱数を受信したＩＣカード内の相互認証部33は、第１の乱数をデータメモリ３２に記憶されている相互認証用暗号コード１を用いてスクランブル化するとともに第１のスクランブル（乱数）、第２の乱数を生成し、データメモリ３２に記憶されている相互認証用暗号コード２を用いてスクラ

ンブル化しデータメモリ３２に記憶する（第２のスクランブル乱数）。さらに、データメモリ３２に記憶されている相互認証用暗号コード１を用いてスクランブル化された乱数と第２の乱数とをICカード用接続端子２３およびインターフェース部４９を介して相互／取引認証部４４に送る。第１のスクランブル乱数と第２の乱数を受信した、相互／取引認証部４４は、第１のスクランブル乱数とメモリ４８に記憶された相互認証用暗号コード１を用いてスクランブル化された乱数１とを比較し、一致した場合には、ＩＣカード１２は、カードターミナル１１と同一の相互認証用暗号コード１を持っていると判断し、相互／取引認証部４４は、ＩＣカード１２を正当なカードとみなして処理を続ける。一致しなかった場合には、ＩＣカード１２は、カードターミナル１１と同一の相互認証用暗号コード１を持っていないと判断し、相互／取引認証部４４は、ＩＣカード１２を不正なカードとみなしてインターフェース部４９を介して中央制御部２２にカードＮＧのメッセージを送信に送る。一致しなかった場合には、カードターミナル１１は、ＩＣカード１２と同一の相互認証用暗号コード２を持っていないと判断し、ＩＣカード内の相互認証部３３は、カードターミナル１１を不正なターミナルとみなして認証ＮＧのメッセージを、ＩＣカード用接続端子２３およびインターフェース部４９を介して相互／取引認証部４４に送る。ステップＳ２において、中央制御部２２は、認証ＮＧのメッセージを受信した場合には、表示制御部４２を介してＬＣＤ１４にエラーを表示し、処理を停止する。認証ＯＫのメッセージを中央制御部２２が受信した場合には、中央制御部２２は、ステップＳ３において、インターフェース部４９およびＩＣカード用接続端子２３を介してＩＣカード１２のデータメモリ３２に記憶されている本システムでの取引手順をよみだし、以下、その手順に従って動作する。本実施例では、暗証入力がＯＫとなった後に、取引認証番号を生成するものとする。

暗証番号の入力が必要な場合、中央制御部２２は、表示制御部４２を介してＬＣＤ１４に、カード所有者に、暗証入力を促すメッセージを表示する。カード所有者は、ステップＳ４において、カードターミナル１１のキー入力部１３より暗証番号ＰＩＮをキー入力する。すると、このキー入力によるＰＩＮデータは、キー入力制御部４１を介して中央制御部２２に入力された後インターフェース部４９およびＩＣカード用接続端子２３を介してＩＣカード内のＰＩＮ照合部３４に送られる。そして、このＰＩＮ照合部３４にてラッチされたキー入力によるＰＩＮデータは、ステップＳ５において、データメモリ３２にてあらかじめ記憶される本カード１２の真の所有者の暗証番号ＰＩＮと比較照合されるので、ここで、キー入力によるＰＩＮと真のＰＩＮとが一致し、上記ステップS1におけるＰＩＮのキー入力者は、本カード１２の真の所有者であると判定されるとステップＳ６に進み中央制御部３１は、カードターミナル１１に対して、本人ＯＫのメッセージを送信する。これにより、カードターミナル１１の表示部１４には、

し、処理を終了する。第１のスクランブル乱数とデータメモリ４８に記憶された、メモリ４８に記憶されている相互認証用暗号コード１を用いてスクランブル化された乱数１とを比較し、一致した場合には、相互／取引認証部４４は、受信した、乱数２をメモリ４８に記憶されている相互認証用暗号コード２を用いてスクランブル化し、インターフェース部４９およびＩＣカード用接続端子23を介してＩＣカード内の相互認証部３３に送る。インターフェース部４９およびＩＣカード用接続端子２３を介して送られた乱数２を受信した、ICカード内の相互認証部３３は、第２の乱数と、データメモリ３２に記憶されている第２のスクランブル乱数と比較し、一致した場合には、カードターミナル１１は、ＩＣカード１２と同一の相互認証用暗号コード２を持っていると判断し、ＩＣカード内の相互認証部３３は、カードターミナル11を正当なターミナルとみなして認証ＯＫのメッセージを、ＩＣカード用接続端子２３およびインターフェース部４９を介して相互／取引認証部４４

表示制御部４２を介して本人ＯＫのメッセージが表示されるようになり、このＯＫメッセージが表示されたままの状態で、カードターミナル１１を商店のオペレータに渡すことにより、オペレータはカード所持者の正当性を確認することができる。

一方、上記ステップＳ６にて、カードターミナル１１に対して、本人ＯＫのメッセージが入力されない場合には、上記表示部１４には、エラーメッセージが表示され、商店オペレータは、上記ＰＩＮ入力者が不正なカード所持者であることを確認することができる。

こうして、カード所有者の正当性が確認されると、商店オペレータは、カードターミナル１１の表示部１４の表示に従い、いずれかのキーを押下する。すると、カードターミナル１１は、取引認証番号生成のためのキー入力待ち状態となる。ここで、商店オペレータは、電話あるいはオンラインアクセスでクレジット会社にクレジット会員番号などの、カード所持者を特定できる情報と、購入金額などの取引を特定できる情報を伝える。クレジット会社では、クレジット会員番号から、クレジット会社で管理している、ＩＣカード１２のデータメモリ３２に記憶されている取引認証番号生成に使用される暗号化コード３と同一のコードを検索し、本コードと、購入金額などの取引を特定できる情報から、取引認証番号生成番号を作り出し、商店オペレータに伝える。商店オペレータは、ステップＳ７において、カードターミナル11のキー入力部１３よりクレジット会社から伝えられた、取引認証番号生成番号を入力する。このキー入力による取引認証番号生成番号は、キー入力制御部４１を介して中央制御部２２に入力された後インターフェース部４９を介して相互／取引認証部４４に、ステップＳ８においてＩＣカード用接続端子２３およびインターフェース部４９を介して読み出されたＩＣカード１２のデータメモリ３２に記憶されている取引認証番号生成に使用される暗号化コード３とともにステップＳ９において取引認証番号生成コマンドとして送られる。相互／取引認証部４４は、取引認証番号生成コマンドにより、ステップＳ１０において取引認証番号生成プログラムを起動し、暗号化コード３にて取引認証番号生成番号をスクランブル化する。このスクランブル化されたデータを、取引認証番号とし、ステップＳ１１においてインターフェース部４９を介して中央制御部２２に入力され、表示制御部４２を介して表示部１４にて表示出力されるようになる。ここで、商店オペレータは、表示出力された取引認証番号を、クレジット会社に伝える。クレジット会社では、暗号化コード３と同一のコードを用いて、取引認証番号生成番号をスクランブル化し、商店オペレータより伝えられた、取引認証番号と比較する。クレジット会社でスクランブル化した取引認証番号生成番号と、カードターミナル１１でスクランブル化した取引認証番号生成番号が一致すれば、クレジット会社は、正当なカード１２を、正当なカードターミナル１１で、正当な所有者が、使用した、正当な取引である、と判断し、商店オペレータに、取り引きの成立を伝える。クレジット会社でスクランブル化した取引認証番号生成番号と、カードターミナル11でスクランブル化した取引認証番号生成番号が一致しなければ、カード１２、または、カードターミナル１１、若しくは、その双方が、不正なものであるので、クレジット会社は、不正な取引であると判断し、商店オペレータに、取り引きの不成立を伝える。

取引が成立した場合、このカード取引認証番号は、各商店ごとに設置されているエンボスインプリンタにより領収書に印字され、カード所有者に渡される。ここで、カード所有者が上記オペレータより渡された領収書にサインをし、ＩＣカードによる取り引きの全過程を終了する。

したがってこのように構成されるオフラインターミナルを用いれば、安全で、確実な、カード取引が、容易に、実現可能となる。

尚、上記実施例においては、取引認証番号をＬＣＤ１４にて表示し、それを、商店オペレータが、クレジット会社に伝えているが、このデータは、例えば、スピーカ２４を介して、ＤＴＭＦ音

として出力してもよい。又、カード所持者の正当性を、ＰＩＮで証明しているが、本オフラインターミナルに、イメージリーダをもうけ、指紋などのイメージ情報にてカード所持者の正当性を証明するようにすれば、システムの安全性は、より高まる。又、記実施例においては、商店での取り引きを例に上げたが、本オフラインターミナルを個人で所有していれば、電話等での通信販売等において利用しても確実に本人確認が可能であるので、サービス提供者、カード所持者、の双方に安全なシステムを提供することが可能となる。

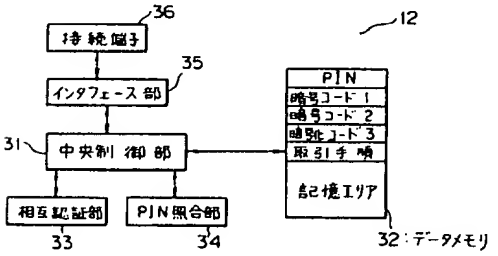
〔発明の効果〕

以上のようにこの発明によれば、予めカード所有者特定用のデータが記憶されるＩＣカードとの電気的接続を図るカード装着部と、売買金額などの取り引きデータを入力するキー入力部をもうけ、カードとカードターミナルの相互認証を行い、上記カード装着部にて接続状態にあるＩＣカードより読み取ったカード所有者特定用のデータと上記キー入力部より入力される取引データに基づきカード取引認証番号を算出し、これを、クレジット会社等で算出した結果と比較するように、構成したので、カードの不正、ターミナルの不正、所持者の不正等を、容易に発見することが可能となり、きわめて安全なカード取引方式を構築することが可能となる。

4．図面の簡単な説明

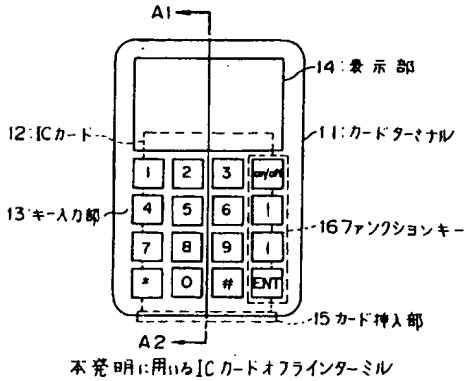
第１図は本発明の取引認証方式に用いるＩＣカードの回路図、第２図は本発明の取引認証方式に用いるＩＣカードオフラインターミナルの概観図、第３図は第２図におけるＡ１－Ａ２線断面図、第４図は本発明の取引認証方式に用いるＩＣカードターミナルの回路図、第５図は本発明の取引認証方式における一実施例のフローチャート。

１１…ＩＣカードターミナル、１２…ＩＣカード、２２，１１…中央制御部、３３，４６…相互認証部、３４…ＰＩＮ照合部、３２，４８…データメモリ。



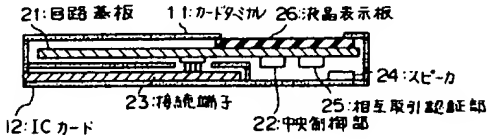
本発明の取引認証方式に用いるICカードの回路図

第１図



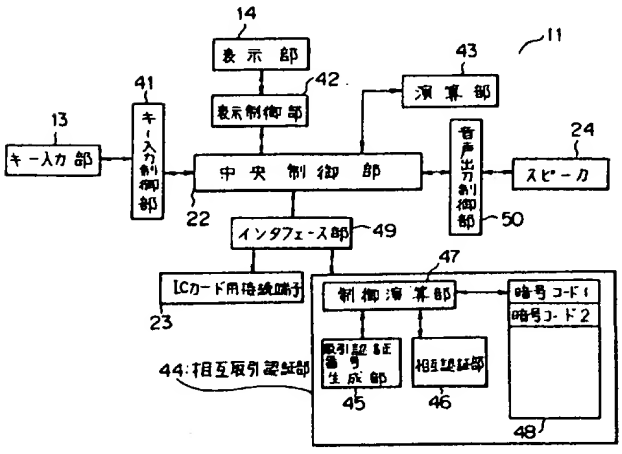
本発明に用いるICカードオフラインターミナル

第２図



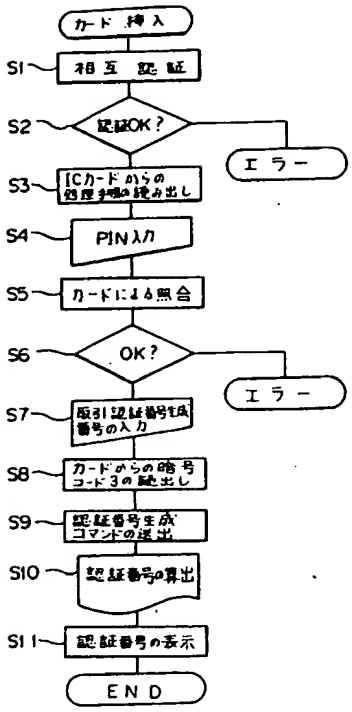
第2図のICカードターミナルのA1-A2断面図

第３図



本発明の取引認証方式に用いるICカードターミナルの回路図

第４図



取引認証方式の動作フローチャート

第 5 図

第1頁の続き

⑤1Int. Cl.⁵	識別記号		庁内整理番号
G 06 F 15/30	340	C	6798−5L
			6798−5L
G 06 K 17/00		S	6711−5L
G 07 F 7/12			